UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/777,550	02/05/2001	David J. Wetherall	41007.P003	8207

29127 7590 12/02/2004

HOUSTON ELISEEVA
4 MILITIA DRIVE, SUITE 4
LEXINGTON, MA 02421

EXAMINER	
PHILLIPS, HASSAN A	

ART UNIT	PAPER NUMBER
2151	

DATE MAILED: 12/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/777,550	WETHERALL ET AL.	
	Examiner	Art Unit	
	Hassan Phillips	2151	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 August 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34 and 36-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34 and 36-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to amendments received on August 6, 2004.

Specification

1. The Examiner has considered the amendments made to the specification. The Examiner has withdrawn all objections to the specification.

Response to Arguments

1. Applicant's arguments filed August 6, 2004 have been fully considered but they are not persuasive.

Applicant argues that:

a) Porras does not teach determining "whether selected instances of source addresses of packets...are spoof source addresses, based at least in part on one or more consistency measures".

Examiner respectfully submits that Applicant has misinterpreted the prior art of record.

Regarding item a), the teachings of Porras clearly shows receiving network packets and building at least one short-term, and one long-term statistical profile from at least one measure of the packets. Suspicious network activity (i.e. spoof source addressing) is then determined by comparing the short-term and long-term profiles.

See col. 1, lines 43-53. The Examiner, as would any one of ordinary skill in the art, has interpreted the comparing of the short-term and long-term profiles to determine suspicious network activity as being a consistency measure determination since suspicious network activity is determined based on how consistent the short-term profile is to the long-term profile. Also see col. 5, lines 4-51.

Furthermore The Examiner has interpreted the claim language as broadly as possible. It is also the Examiner's position that Applicant has not yet submitted claims drawn to limitations, which define the operation and apparatus of Applicant's disclosed invention in a manner that distinguishes over the prior art.

Failure for Applicant to significantly narrow definition/scope of the claims implies the Applicant intends broad interpretation be given to the claims. The Examiner has interpreted the claims with scope parallel to the Applicant in the response and reiterated the need for Applicant to define the claimed invention more clearly and distinctly. Accordingly the references supplied by the examiner in the previous office action covers the claimed limitations. The rejections are thus sustained. Applicant is requested to review the prior art of record for further consideration.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) The invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the

applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-34, 36-48 are rejected under 35 U.S.C. 102(e) as being anticipated by Porras et al. (hereinafter Porras), U.S. patent 6,321,338.

3. In considering claim 1, Porras discloses a network comprising:

a) A plurality of network nodes, (see Fig. 1);

b) A plurality of routing devices to route network traffic between network nodes, (col. 3, lines 44-45);

c) A director coupled to the routing devices to determine whether selected instances of source addresses of packets routed by the routing devices are spoof source addresses, based on consistency measures, (col. 1, lines 43-53).

4. In considering claim 2, the method of Porras provides a means for determining whether selected instances of source addresses of packets routed by the routing devices are spoof source addresses, based on spatial distribution profiles of source addresses in view of a reference source address spatial distribution profile. See col. 5, lines 36-51.

5. In considering claim 3, the method of Porras provides a means for the reference source address spatial distribution profile to comprise a historical spatial distribution profile for a particular address. See col. 5, lines 38-40.

6. In considering claim 4, the method of Porras provides a means for determining whether selected instances of source addresses of packets routed by the routing devices are spoof source addresses, based on destination source address range (DSAR) distribution profiles of the source addresses in view of a reference DSAR distribution profile. See col. 5, lines 36-51.

7. In considering claim 5, the method of Porras provides a means for the reference DSAR distribution profile to comprise a historical DSAR distribution profile for a particular address. See col. 5, lines 38-40.

8. In considering claim 6, the method of Porras provides a means for determining whether selected instances of source addresses of packets routed by the routing devices are spoof source addresses, based on migration distribution profiles of source addresses in view of a reference source address migration distribution profile. See col. 5, lines 36-51.

9. In considering claim 7, the method of Porras provides a means for the reference source address migration distribution profile to comprise a historical migration distribution profile for a particular address. See col. 5, lines 38-40.

10. In considering claim 8, the method of Porras provides a means for determining whether selected instances of source addresses of packets routed by the routing devices are spoof source addresses, based on timing distribution profiles of source addresses in view of a reference source address timing distribution profile. See col. 5, lines 36-51.

11. In considering claim 9, the method of Porras provides a means for the reference source address timing distribution profile to comprise a historical timing distribution profile for a particular address. See col. 5, lines 38-40.

12. In considering claim 10, the method of Porras teaches the director being equipped to determine whether filtering actions are to be taken amongst particular routing devices. See col. 9, lines 57-63.

13. In considering claim 11, it is inherent in the method of Porras that the director takes into consideration, when making its determination, whether packets of non-spoof instances of a source address having instances deemed to be spoof source addresses are likely to be routed in the network. See col. 9, lines 57-63.

14. In considering claim 12, the method of Porras teaches a plurality of director devices cooperatively coupled to each other to jointly make determinations. See col. 3, lines 16-40.

15. In considering claim 13, the method of Porras further teaches a plurality of sensors for monitoring and reporting source addresses of packets routed through routing devices. See col. 3, lines 42-45.

16. In considering claim 14, the method of Porras further teaches sensors facilitating application of the desired source address based filtering on packets being routed through the routing devices. See col. 3, lines 55-65.

17. In considering claim 15, Porras discloses a networking method comprising:

a) Receiving information associated with source addresses of packets being routed to and from a plurality of network nodes, and determining whether selected instances of the source addresses are spoof instances based on consistency measures, (col. 1, lines 43-53);

b) Managing the network based, at least in part, on the results of the determination, (col. 1, lines 66-67, col. 2, lines 1-7).

18. In considering claim 16, the method of Porras provides a means for determining whether selected instances of source addresses of packets are spoof source addresses, based on spatial distribution profiles of source addresses in view of a reference source address spatial distribution profile. See col. 5, lines 36-51.

19. In considering claim 17, the method of Porras further provides a means for constructing the spatial distribution profiles. See col. 5, lines 4-36.

20. In considering claim 18, the method of Porras further provides a means for determining whether each of the spatial distribution profiles is within a resemblance tolerance limit when compared to each of the at least one reference source address spatial distribution profiles. See col. 5, lines 38-40.

21. In considering claim 19, the method of Porras provides a means for the reference source address spatial distribution profile to comprise a historical spatial distribution profile for a particular address. See col. 5, lines 38-40.

22. In considering claim 20, the method of Porras provides a means for determining whether selected instances of source addresses of packets are spoof source addresses, based on DSAR distribution profiles of source addresses in view of a reference source address DSAR distribution profile. See col. 5, lines 36-51.

23. In considering claim 21, the method of Porras further provides a means for constructing the DSAR distribution profiles. See col. 5, lines 4-36.

24. In considering claim 22, the method of Porras further provides a means for determining whether each of the DSAR distribution profiles is within a resemblance tolerance limit when compared to each of the at least one reference source address DSAR distribution profiles. See col. 5, lines 38-40.

25. In considering claim 23, the method of Porras provides a means for the reference source address DSAR distribution profile to comprise a historical DSAR distribution profile for a particular address. See col. 5, lines 38-40.

26. In considering claim 24, the method of Porras provides a means for determining whether selected instances of source addresses of packets are spoof source addresses, based on migration distribution profiles of source addresses in view of a reference source address migration distribution profile. See col. 5, lines 36-51.

27. In considering claim 25, the method of Porras further provides a means for constructing the migration distribution profiles. See col. 5, lines 4-36.

28. In considering claim 26, the method of Porras further provides a means for determining whether each of the migration distribution profiles is within a resemblance

tolerance limit when compared to each of the at least one reference source address migration distribution profiles. See col. 5, lines 38-40.

29. In considering claim 27, the method of Porras provides a means for the reference source address migration distribution profile to comprise a historical migration distribution profile for a particular address. See col. 5, lines 38-40.

30. In considering claim 28, the method of Porras provides a means for determining whether selected instances of source addresses of packets are spoof source addresses, based on timing distribution profiles of source addresses in view of a reference source address timing distribution profile. See col. 5, lines 36-51.

31. In considering claim 29, the method of Porras further provides a means for constructing the timing distribution profiles. See col. 5, lines 4-36.

32. In considering claim 30, the method of Porras further provides a means for determining whether each of the timing distribution profiles is within a resemblance tolerance limit when compared to each of the at least one reference source address timing distribution profiles. See col. 5, lines 38-40.

33. In considering claim 31, the method of Porras provides a means for the reference source address timing distribution profile to comprise a historical timing distribution profile for a particular address. See col. 5, lines 38-40.

34. In considering claim 32, the method of Porras teaches, in managing the network, determining whether filtering actions are to be taken amongst particular routing devices. See col. 9, lines 57-63.

35. In considering claim 33, it is inherent in the method of Porras when making the determination, to take into consideration whether packets of non-spoof instances of a source address having instances deemed to be spoof source addresses are likely to be routed in the network. See col. 9, lines 57-63.

36. In considering claim 34, Porras discloses an apparatus comprising:

a) A storage medium having stored therein a plurality of programming instructions designed to implement a director to receive reporting of information associated with source addresses of packets routed through a plurality of routing devices of a network, and to determine whether at least some instances of the source addresses are spoof instances based on spatial distribution profiles of source addresses and in view of at least one reference source address spatial distribution profile, and a processor

coupled to the storage medium to execute the programming instructions, (col. 2, lines 25-35, also see col. 5, lines 36-51).

37. In considering claim 36, the apparatus of Porras further provides a means for constructing the spatial distribution profiles. See col. 5, lines 4-36.

38. In considering claim 37, the apparatus of Porras further provides a means for determining whether each of the spatial distribution profiles is within a resemblance tolerance limit when compared to each of the at least one reference source address spatial distribution profiles. See col. 5, lines 38-40.

39. In considering claim 38, the apparatus of Porras provides a means for determining whether selected instances of source addresses of packets are spoof source addresses, based on DSAR distribution profiles of source addresses in view of a reference source address DSAR distribution profile. See col. 5, lines 36-51.

40. In considering claim 39, the apparatus of Porras further provides a means for constructing the DSAR distribution profiles. See col. 5, lines 4-36.

41. In considering claim 40, the apparatus of Porras further provides a means for determining whether each of the DSAR distribution profiles is within a resemblance

tolerance limit when compared to each of the at least one reference source address DSAR distribution profiles. See col. 5, lines 38-40.

42. In considering claim 41, the apparatus of Porras provides a means for determining whether selected instances of source addresses of packets are spoof source addresses, based on migration distribution profiles of source addresses in view of a reference source address migration distribution profile. See col. 5, lines 36-51.

43. In considering claim 42, the apparatus of Porras further provides a means for constructing the migration distribution profiles. See col. 5, lines 4-36.

44. In considering claim 43, the apparatus of Porras further provides a means for determining whether each of the migration distribution profiles is within a resemblance tolerance limit when compared to each of the at least one reference source address migration distribution profiles. See col. 5, lines 38-40.

45. In considering claim 44, the apparatus of Porras provides a means for determining whether selected instances of source addresses of packets are spoof source addresses, based on timing distribution profiles of source addresses in view of a reference source address timing distribution profile. See col. 5, lines 36-51.

46. In considering claim 45, the apparatus of Porras further provides a means for constructing the timing distribution profiles. See col. 5, lines 4-36.

47. In considering claim 46, the apparatus of Porras further provides a means for determining whether each of the timing distribution profiles is within a resemblance tolerance limit when compared to each of the at least one reference source address timing distribution profiles. See col. 5, lines 38-40.

48. In considering claim 47, the method of Porras teaches instructions designed to be able to determine whether filtering actions are to be taken amongst particular routing devices. See col. 9, lines 57-63.

49. In considering claim 48, it is inherent in the method of Porras that the programming instructions are designed to take into consideration whether packets of non-spoof instances of a source address having instances deemed to be spoof source addresses are likely to be routed in the network. See col. 9, lines 57-63.

Conclusion

1. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

2. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hassan Phillips whose telephone number is (571) 272-3940. The examiner can normally be reached on M-F 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Zarni Maung can be reached on (571) 272-3939. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZARNI MAUNG
PRIMARY EXAMINER